DETERRING CYBERTRESPASS
AND SECURING CYBERSPACE:
LESSONS FROM UNITED STATES BORDER
CONTROL STRATEGIES

Mary Manjikian

The United States Army War College

The United States Army War College educates and develops leaders for service at the strategic level while advancing knowledge in the global application of Landpower.

The purpose of the United States Army War College is to produce graduates who are skilled critical thinkers and complex problem solvers. Concurrently, it is our duty to the U.S. Army to also act as a "think factory" for commanders and civilian leaders at the strategic level worldwide and routinely engage in discourse and debate concerning the role of ground forces in achieving national security objectives.

The Strategic Studies Institute publishes national security and strategic research and analysis to influence policy debate and bridge the gap between military and academia.

The Center for Strategic Leadership contributes to the education of world class senior leaders, develops expert knowledge, and provides solutions to strategic Army issues affecting the national security community.

The Peacekeeping and Stability Operations Institute provides subject matter expertise, technical review, and writing expertise to agencies that develop stability operations concepts and doctrines.

The School of Strategic Landpower develops strategic leaders by providing a strong foundation of wisdom grounded in mastery of the profession of arms, and by serving as a crucible for educating future leaders in the analysis, evaluation, and refinement of professional expertise in war, strategy, operations, national security, resource management, and responsible command.

The U.S. Army Heritage and Education Center acquires, conserves, and exhibits historical materials for use to support the U.S. Army, educate an international audience, and honor Soldiers—past and present.

STRATEGIC STUDIES INSTITUTE

The Strategic Studies Institute (SSI) is part of the U.S. Army War College and is the strategic-level study agent for issues related to national security and military strategy with emphasis on geostrategic analysis.

The mission of SSI is to use independent analysis to conduct strategic studies that develop policy recommendations on:

- Strategy, planning, and policy for joint and combined employment of military forces;

- Regional strategic appraisals;

- The nature of land warfare;

- Matters affecting the Army's future;

- The concepts, philosophy, and theory of strategy; and,

- Other issues of importance to the leadership of the Army.

Studies produced by civilian and military analysts concern topics having strategic implications for the Army, the Department of Defense, and the larger national security community.

In addition to its studies, SSI publishes special reports on topics of special or immediate interest. These include edited proceedings of conferences and topically oriented roundtables, expanded trip reports, and quick-reaction responses to senior Army leaders.

The Institute provides a valuable analytical capability within the Army to address strategic and other issues in support of Army participation in national security policy formulation.

Strategic Studies Institute
and
U.S. Army War College Press

DETERRING CYBERTRESPASS
AND SECURING CYBERSPACE:
LESSONS FROM UNITED STATES BORDER
CONTROL STRATEGIES

Mary Manjikian

December 2016

*****

*****

*****

*****

FOREWORD

For most military analysts, the term "deterrence" brings to mind the notion of nuclear deterrence. We think of how two opposing states attempt to deter their adversaries through creating a balance of weapons, telegraphing their intentions, and establishing themselves as a credible threat. We think of the Cold War, and the standoff between the Soviet Union and the United States.

However, in this Letort Paper, Dr. Mary Manjikian raises the intriguing notion that the best analogy when thinking about cyber-deterrence does not actually come from the nuclear arena but rather from the literature about border controls. Drawing on a rich literature, including case studies of successful and unsuccessful attempts at securing the Southern border of the United States, she demonstrates that the approaches, strategies, and costs of carrying out physical border defense and virtual border defense have many similarities. First, Dr. Manjikian argues that the actors we most need to deter in cyberspace are often not states but rather may include a broad coalition of threats—including insiders, state and nonstate actors, and members of a criminal element. Just as is the case when we consider our physical borders, not everyone who attempts to traverse our virtual borders uses the same methods, nor do they have the same intentions. Thus, differentiated deterrence strategies can be framed and used, depending on the nature of the threat and the adversary's intentions.

Furthermore, Dr. Manjikian argues that in cyber-deterrence, there is no clear moment of a "standoff" between two opposing sides—as we often see in the
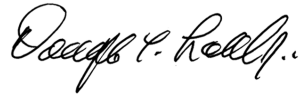
nuclear arena. Instead, the actions taken by those attempting to defend borders in cyberspace and those who attempt to trespass them are ongoing.

In addition, just as is the case in real space-border incursions, over time trespassers learn more about their adversaries' defenses. Each time they make an incursion across the border they gain new information about how resources are organized, where they are deployed, and where the weak points in our defense are. Thus, each incursion—even when unsuccessful—ups the chances that the next incursion will succeed. Moreover, the costs of defense often are significantly greater than the costs of mounting another incursion. Over time, the trespasser's costs may decrease, while the defender's costs remain constant.

Perhaps most significantly, Dr. Manjikian explains why disparate elements who share a border will not always work together to defend that border. In considering physical borders, building a wall or setting up a checkpoint in one location may simply cause those seeking entry to move on to consider a different entry point, which is not as well defended. Similarly, both corporations and agencies may unwittingly create security threats for other agencies or corporate rivals through adopting a more stringent defense of their own borders.

This analysis raises interesting questions and will give readers much to consider in thinking through the issue of cyber-deterrence today. This novel approach

will also, I hope, lead to the creation of novel solutions as we address the growing threat of cybertrespass today.

DOUGLAS C. LOVELACE, JR.
Director
Strategic Studies Institute and
    U.S. Army War College Press

ABOUT THE AUTHOR

MARY MANJIKIAN is Associate Dean of the Robertson School of Government at Regent University. She previously served as a U.S. Foreign Service officer in The Netherlands, Russia, and Bulgaria, and as a Fulbright Scholar at Durham University's Institute of Advanced Study. Dr. Manjikian's publications include *Apocalypse and Post-Politics: The Romance of the End* (Lexington Books, 2012); *Threat Talk: Comparative Politics of Internet Addiction in China and the US* (Ashgate, 2012); and *Securitization of Property Squatting in Western Europe* (Routledge, 2013). Her articles have also appeared in such journals as *International Studies Quarterly*, *International Journal of Intelligence and Counterintelligence*, *Intelligence and National Security*, and *International Feminist Journal of Politics*. Dr. Manjikian holds an M.Phil. from Oxford University and a Ph.D. from the University of Michigan.

SUMMARY

In recent years, analysts have begun discussing strategies for securing entities in cyberspace—including the files and software belonging to corporations, government institutions, and private individuals. Increasingly, analysts have suggested utilizing two types of deterrence strategies: deterrence by denial and deterrence by punishment. In determining how both deterrence strategies might be applied to preventing hostile individuals, states, and nonstate actors from entering cyberspace and inflicting damage there, analysts have borrowed from deterrence strategies that have been framed for a variety of other situations. While the tendency among members of the military community is to look to other military situations—such as nuclear war, or the use of biological or chemical weapons—in which deterrence strategies may have been used, it is my contention that these scenarios are not necessarily the best fit for describing what happens in cyberspace. Rather, my intent in this Letort Paper is to look at other literature that refers to deterrence strategies—namely, criminology literature, which looks at strategies and tactics for deterring illegal immigration.

In the first section of this Letort Paper, three possible strategies for responding to criminal behavior as presented in the criminology literature are described, including: prevention by design; deterrence by denial; and deterrence by punishment. Moreover, this Letort Paper suggests that cyber-deterrent strategies are more properly categorized as prevention by design strategies rather than deterrence by denial strategies, and the difference between the two is explained.

The second section points to existing problems of applying the theories regarding nuclear deterrence to the cyberconflict situation—focusing in particular on the knowledge problem (the problem of attribution) and the temporal problem (the ways in which time functions in cyberspace), both of which are spelled out in greater detail in that section.

The third section explains what can be learned from the criminology example of providing border security. In the border security case, we are able to see how different types of would-be aggressors are approached differently, how targeted strategies are created, and how border security is an issue that needs to be handled in association with related issues, including economic ones. Then, the section examines the ways in which the United States has been able to work with its neighbors in creating border security.

Finally, the concluding section of this Letort Paper draws on the border security example to develop lessons for the provision of cybersecurity.

DETERRING CYBERTRESPASS AND SECURING CYBERSPACE: LESSONS FROM UNITED STATES BORDER CONTROL STRATEGIES

I. THREE TYPES OF CRIMINAL DETERRENT STRATEGIES: PREVENTION BY DESIGN; DETERRENCE BY DENIAL; AND DETERRENCE BY PUNISHMENT

As noted, the concept of deterrence does not belong solely to military and strategic studies scholars. Indeed, there is an equally broad literature about deterrence within the fields of criminology and even the health sciences. In those contexts, analysts consider the ways in which individuals and sometimes groups may be induced to alter or desist in their harmful behaviors through a combination of deterrence by denial and deterrence by punishment strategies. Analysts have asked how individuals and groups may be deterred from engaging in activities such as driving while intoxicated,[1] dealing in illegal drugs,[2] or battering their spouse or significant other.[3]

The criminological model of deterrence and the work done by academic criminologists on practices of deterring offenders provide many useful lessons for those interested in understanding more about the ways deterrence can and does work in cyberspace. As Lynn Zimmer suggests in her work on deterring drug trafficking in American cities, criminal deterrence strategies ideally seek to accomplish two goals. The first is that they are concerned with capturing and sometimes preempting offenders to make sure that they do not offend and re-offend. However, deterrence strategies are also important for creating order within a region or a neighborhood. By "cracking down" on

those who seek to engage in activities that are violent and disruptive to the community as a whole, a collective good—stability and peace—is distributed to the entire community.[4] This same pattern holds true in cyberspace: U.S. cyber-deterrence initiatives, as well as those deterrence initiatives carried out by other states and even corporations within cyberspace, seek to preempt or prevent the carrying out of costly, dangerous, and disruptive attacks against government and civilian critical infrastructure. However, these deterrence initiatives also seek to preserve the peace, stability, and order of cyberspace so that the benefits of the Internet may be enjoyed by all citizens.[5] That is, criminological literature explicitly acknowledges the fact that deterrence is not simply an elite strategy, practiced by elites and affecting only elites within the system. Rather, deterrence is a way of securing space for all citizens within the community.

In addition, the criminology literature—particularly the literature about illegal immigration—focuses on the actors involved in these activities. As Frank Cilluffo *et al.* noted, the nuclear deterrence analogy might not be a good fit with the cyber-deterrence puzzle because its overwhelming focus is on hardware—the weapons that are used to demonstrate resolve. However, Cilluffo *et al.* argued that the real threat in cyberspace comes not from the code itself, but rather from the individuals and groups (including criminal elements, state-sponsored terrorists, and foreign militaries) who seek to use code and computer exploits (actions that take advantage of a computer bug or vulnerability) to enter and destroy parts of cyberspace. Thus, they argue, the key to defeating these intrusions lies not in focusing on weapons but on the individuals and groups who use them—through a

better understanding of their motivations, views, and conceptualizations of risk and threat.[6] It therefore may be more useful to ask: "How do deterrence strategies prevent individuals from driving while intoxicated, from engaging in domestic violence, or from engaging in illegal immigration—and what can we learn from these situations that is relevant to the best ways to deter cyber-intruders rather than to dwell at length on specific technological specifications and their effects on driving or ending the cyber-arms race?"

In addition, the literature on deterring criminal behavior does not assume—as nuclear deterrence writing does—that motives are unalterable and incapable of being changed. Looking predominantly at individual law-breaking behavior, this literature pays more attention to the way individuals make choices to engage in behavior the authorities wish to deter, as well as the circumstances that might create these behaviors to begin with. For example, a study of driving while intoxicated does not consider merely what remedies are most effective in reducing or deterring the behavior, but may also engage with the "why questions"— the reasons some deterrent strategies work better than others. Another "why question" could be the degree to which a penalty for drunk driving might lead to a cessation of the behavior, rather than merely a decision to engage in the behavior in another state where perhaps penalties are less strict. That is, the strategy does not take preferences as given, but also asks how preferences might be changed.[7]

Furthermore, the criminological literature on deterrence is in some ways much richer than that about nuclear deterrence, which cyber-analysts have thus far devoted the bulk of their attention to. Because there are so many instances of crimes, such as illegal

immigration, drug trafficking, or driving under the influence—and so few cases of nuclear launches—there are a much wider variety of cases of both successful and failed deterrence efforts for analysts to examine. Because the emphasis is on understanding a mass rather than an elite phenomenon, we have the opportunity to use methodologies to study the problem that would not be available in studying nuclear deterrence, for example. In particular, as this Letort Paper indicates, there are numerous studies of illegal immigration based on survey data and interviews collected from both failed and successful illegal immigrants. This data allows us to speak at greater length about the individual psychological decision-making processes, which individuals undergo in reacting to a deterrent, as well as to understand better which types of deterrents are more or less successful in preventing an attack. The criminology literature is also much more explicit about the end goals sought in utilizing deterrence strategies. Analysts ask, "Do we want to reform the criminal, to cause him not to engage in criminal behavior anymore, or merely prevent him from robbing my house?" In each case, the action is deterred, but the result is somewhat different, not only for the person implementing the strategies but for his or her neighbors as well.

What Can Studies of Drunk Drivers Teach Us About Cyber-Deterrence?

Valid lessons can be culled from examining surveys of would-be immigrants in particular to help us understand how potential cyber-aggressors think about issues, including strategy, tactics, targeting, and the likelihood of success and failure. In presenting

both nuclear deterrent and criminal deterrent strategies, analysts rely on certain assumptions about how individuals make decisions, based on the notion of the rational actor. In each case, analysts assume that the actor who is deciding whether to act is aware of his or her preferences; that he or she is able to state those preferences and to rank-order them; and that he or she is aware of the costs and benefits (the utility) associated with these preferences. Models also assume that deterrence strategies can be effective in changing the actions of individuals and groups, and that outside analysts are able to interpolate the actors' preferences to assign value to and rank them and to rank the preferred options and outcomes of each side in the conflict.

Within criminology literature, analysts distinguish between not two but three different types of deterrent strategies. The first is **deterrence**, **or prevention by design**. In these cases, analysts may assume that the behavior they are trying to prevent is not ultimately preventable, because of human nature, social practices, or another variable. In such cases, a decision is made that it is not cost-effective—or perhaps not even possible—to seek to change individual's preferences and practices. Therefore, officials may decide not to spend time and money on convincing individuals not to deface public property, not to engage in prostitution, or not to text and drive. Instead, they may work with designers, architects, or even medical personnel to put measures in place that make the individual unable to engage in his or her desired action regardless of his or her preferences. Design modifications—or barriers— might include requiring sex offenders to take medication that makes sexual activity impossible; developing special repellent paints to use in public places that

make producing graffiti impossible; or constructing a physical structural wall between bordering nations to make illegal immigration impossible. [8] Indeed, the design of many computer firewalls is properly understood as a form of prevention by design.

Although such designs may be highly effective, it is worth noting that adopting such strategies has its limitations, since it **does not actually change the preference structure of the would-be offender, nor does it establish community norms against the behavior.** Instead, prevention by design strategies often **merely stem a particular set of behaviors at a particular geographic location.** However, since the strategies do not change preferences, it is likely that the would-be offenders will simply move on to perform the undesirable behavior at a different location. For example, a business that plays old-fashioned music to discourage teens from loitering outside the establishment has not actually solved the problem of loitering but has only encouraged the teens to move on to a different location or target.

In addition, prevention by design can be seen as a dynamic process. It is unlikely that the "architects" of this policy will ever arrive at a perfect solution that prevents all of the unwanted behaviors. Instead, one can envision a scenario in which would-be rule violators design a work-around to lessen the effects of the prevention by design measure. (For example, undocumented immigrants wishing to enter the United States but encountering a border fence might choose another location to make their entrance attempt, or they might hire a more experienced guide to assist them in their efforts.) Thus, any investment in prevention by design is likely to be temporary or of limited value. It is not a permanent solution. This understanding presents a dilemma—since the creation of a prevention by design

strategy may necessitate a long-term investment by an actor to secure what is perhaps only a short-term advantage.

Here, the lesson for cybersecurity is clear as well. Barriers that prevent actors from accessing a system need to be, as Emilio Iasiello notes, "relentlessly monitored and adapted to a constantly changing threat environment."[9] Here we can consider events in 2014 and 2015, in which much of the energy in cyber-defense and cyber-deterrence was aimed at improving the security of major corporations (like those associated with credit cards and the financial system), which succeeded only in leaving additional vulnerabilities open, such as the possibility that hackers would then target the healthcare industry.

Prevention by design strategies are also unusual in that they are most often "one size fits all." strategy. It is harder to come up with a targeted prevention by design strategy, since most often design modifications will prevent **all** affected actors from engaging in the action in all situations, rather than merely preventing some individuals in some situations. For example, a municipality that designs a town square without seating in order to prevent homeless individuals from taking up residence in the square will not succeed in preventing only this action. Rather, it is just as likely that the disabled or elderly visitor to the square will also have nowhere to sit. (Similarly, an Internet filter meant to prevent schoolchildren from accessing sexual content might also affect the adults working at the school, preventing them from, for example, preparing a biology lesson.) Prevention by design strategies are, in this regard, crude but highly effective strategies.

Table 1 illustrates how prevention by design strategies work in three areas—criminology, law enforcement, and cybersecurity.

Field	Action	Prevent by Design Strategy	Possible Outcomes
Criminology:	Driving While Intoxicated	Install devices like breathalyzers in cars to prevent individuals from driving while drunk	Individual may decide not to drive while drunk, OR he may procure another vehicle
Law Enforcement:	Overcoming Border Security	Install fences along U.S. southern border	Individual may decide not to immigrate, or may continue to make repeated attempts, often at other locations
Cybersecurity:	Unauthorized Access to systems	Use of firewalls	Individual may decide not to access and may move on, choosing a different target

Table 1. Prevention by Design Strategies.

Writing about cyber-deterrence frequently conflates together the notion of prevention by design and deterrence by denial, since this distinction is not as clear in the international relations literature as it is in the criminology literature. In particular, proponents of cyber-deterrent strategies may speak of raising the costs of attack, stating that an adversary may preemptively decide not to attack a target because the perceived costs of attack are too high due to the information available about the barriers that must be accessed surrounding the target. Thus, they draw on the writings of the military strategist Sun Tzu, who suggested

that the best conflict is the one you are never forced to fight because your opponent is intimidated and withdraws before war is declared.

In point of fact, one can raise the costs of an attack either through design modifications—such as a border fence, which would be expensive to scale without elaborate equipment or outside help—or through a deterrence by denial strategy, such as export controls, which would make it difficult for an adversary to assemble the necessary components to carry out an attack. Here, deterrence by denial refers to the creation of barriers to entry, which would raise the costs and level of difficulty experienced by would-be hackers seeking to access information or assets through cyberspace. In such a circumstance, the expectation is either that the would-be attackers would fail in their attempts, or that they would preemptively decide not to attack, based on what they know about their odds of success and failure. (That is, their preferences might actually be changed.)

For example, an opponent who contemplates assembling a nuclear weapon might be prevented from doing so through a concerted effort by all nations within the international community not to allow rogue nations to buy enriched uranium or acquire the laboratory equipment and technical expertise needed. Here, a multilateral combination of monitoring, export controls, and intelligence activities is used together to deny the adversary access to the necessary components. Deterrence by denial strategies may thus rest on a strategy of publicity in which would-be attackers or lawbreakers are made aware in advance of the barriers to their access, or they may be carried out covertly, with would-be attackers becoming aware of the barriers only when they encounter them through

actions. Braun and Chyba (2004) refer to such a regime as a "supply side strategy," since the aim is to keep would-be aggressors from procuring the necessary supplies to carry out their attacks.[10] Similarly, Barnum distinguishes between "inward-looking strategies," which ask the defender to consider what his or her own weaknesses or points of vulnerability might be, and "outward-looking strategies," which might consider the resources that the community as a whole has to defeat the aggressor.[11]

While the two strategies—prevention by design and deterrence by denial—might look similar on the surface, they are not in fact the same strategy. Both are strategies that require planning and intelligence. Those who seek to prevent an action or deny an adversary are in both cases acting on information they already have on what the adversary is likely to do. In this way, both strategies are proactive, rather than reactive.[12] However, prevention through design is a unilateral strategy that any individual player could mount. It does not require any outside cooperation to work, nor does it create any form of community good. In contrast, deterrence through denial may be carried out either unilaterally or multilaterally.[13] In a multilateral deterrence strategy, the actors wishing to deter an action may cooperate to establish a regime in order to create a community good (such as international security). A multilateral strategy would require a "buy-in" from other actors within a neighborhood or international community.

Analysts also differ as to whether deterrence by denial strategies are effective in changing the preferences of the would-be aggressor. In criminology terms, consider a strategy aimed to deter underage drinking through requiring proper identification for those

wishing to enter an establishment serving or selling alcohol (deterrence by denial), as well as through punishing those caught with illegal possession of alcohol (deterrence by punishment). It is possible that requiring proper identification would deter some individuals who sought illegal access to alcohol, while others might go around the prohibition by procuring a false identification card.[14]

Also, consider the example of international export control regimes aimed at deterring rogue states and nonstate actors from securing access to chemical, biological, or nuclear weapons. While some actors might be deterred by the difficulties erected through such regimes, others might be more persistent—and instead of abandoning the quest, they might turn to other suppliers for the needed ingredients. Alternately, they might choose another tactic for launching their attack, such as, for example, a suicide attack over a biological weapons attack.

It is my contention that in discussing cybersecurity initiatives, many examples of prevention through design approaches have actually been mislabeled as deterrence by denial. While it is true that today the United States is involved in multilateral efforts to secure cyberspace and to deter aggressors, it is equally true that corporations overwhelmingly provide only for their own cybersecurity and that they are reluctant to provide information about either the attacks that they have undergone or those that they have prevented in the larger community. The majority of cybersecurity initiatives today—particularly those undertaken by corporate actors—are unilateral, aimed not at securing a public good, such as a more secure cyberspace, but rather, securing the "borders" of particular corporations, even if doing so means increasing the likeli-

hood that the same actor might target another American entity. In each case, the aim of the protector is not to change the strategy or practices of the aggressor, but instead, merely to prevent incursion into one's own system. In Realist terms, one could argue that prevention by design is a selfish strategy, in which an organization prioritizes its own survival over that of the collective. A graphic example of this strategy in practice would be a situation in which New Mexico, for example, became a stringent enforcer of border security, thus leading to more individuals attempting to cross the border into California.[15]

SUGGESTIONS FOR PLANNERS

In considering how organizations such as U.S. Cyber Command might work with corporations to prevent unauthorized access to both corporate information and specifically, customer information belonging to U.S. citizens, it is thus important to consider the difference between the two strategies—prevention by design versus deterrence by denial. One can draw the following lessons from looking at prevention by design strategies:

- Do not assume that attackers will eventually "learn" anything, including the futility of mounting future attacks.
- Do not expect that any form of community or shared interests would evolve among organizations predominantly utilizing a prevention by design approach.
- When one player increases its prevention by design level, the costs may be passed on to other organizations, which now become more attractive targets. The "arms race" created is thus

not between the attacker and the target, but between multiple targets, each of whom wants to be seen as the least desirable, most difficult, or most expensive site for attack.[16]

- Cyber-deterrent barriers need to be dynamic. The dilemma is that a long-term investment may be required to produce only a short-term advantage.

Table 2 illustrates differences between prevention by design and deterrence by denial.

	Prevention by Design	Deterrence via Denial
Goal:	Raise costs, barriers to attack	Raise costs, barriers to attack
Actors:	Individual (corporation, municipality, etc.)	Individual or Community
Goods Created:	Individual Goods	Individual or Community Goods
Who Is Deterred?	Everyone	The least persistent actors
Desired Actions:	Attacker will choose new target	Attacker will decide not to attack or choose new target or strategy

Table 2. Prevention by Design vs. Deterrence by Denial.

The final deterrent strategy that criminologists refer to in their work is deterrence by punishment. This term refers to strategies that would be implemented to punish individuals and groups, and in some cases, their sponsors (including state sponsors), once access has been detected and, in some cases, damage has been sustained. While both prevention by design and deterrence by denial are proactive strategies aimed at preventing a breach from occurring, deterrence by

punishment refers to actions taken after a breach has occurred. However, one can also deter based on a threat of punishment—in essence effecting the calculations that the would-be attacker carries out before deciding not to attack based on the likely punishment for doing so. That is, one can preempt conflict through the creation of an expectation that the punishment received for one's attempt is far greater than any gain one could possibly expect to receive through that attempt.

Here, criminologists and military thinkers part ways in their analysis of deterrence by punishment. Theorists within military ethics and international law are particularly preoccupied with the size of the threatened punishment, which is threatened, and they have argued about whether deterrence by punishment necessarily rests on a use of disproportionate force in relation to the action itself—a situation that would seem to violate the international law principle of proportionality.[17] In addition, analysts who write about nuclear deterrence speak of a punisher's resolve and credibility: consider, for example, whether the Soviet Union really believed that the United States would be willing to inflict a nuclear strike during the Cold War era.

In contrast, criminologists have focused on the deterrent effects of punishment, focusing not on the punishment itself but on the way the would-be aggressor understands that punishment. They have asked whether young miscreants are sufficiently well informed about the punishment they are likely to receive, and how clearly the signal regarding their likely punishment has been received. Findings of a study about drinking and driving among college students found that the best predictors of an effective deter-

rence by punishment strategy were the "celerity" and imminence of the threatened punishment along with the certainty and severity of that punishment. The same study found that individuals might be as affected by the extra-legal consequences of a punishment as they are by the legal ones.[18] Here again the criminology literature is more nuanced, distinguishing between serial recidivists and one-time offenders. In this way, the criminology literature enables us to examine situations of iterated deterrence, which have not merely one deterrent event but several. As argued in Section II of this Letort Paper, the iterative nature of cyberattacks is one key feature that distinguishes cyber-conflict from more traditional military conflict, including nuclear conflict.

II. WHY THE NUCLEAR ANALOGY IS A BAD FIT

As noted, most queries regarding how deterrence might be applied in cyberspace thus far have been based on an analysis of the literature on nuclear deterrence.[19] Analysts have asked whether it might be possible to draw a "red line" in cyberspace, or set up conditions under which aggressors would become aware that their actions were subject to deterrence by punishment.[20] They have also described the ways in which the "battlespace" has been secured through the use of nuclear weapons, and asked whether cyberweapons, along with more conventional weapons, could not play a similar role in defending the cyber-battlespace.[21] Parallels are frequently drawn between the mutually assured destruction (MAD), which would be created if both sides were to use nuclear weapons in a bilateral conflict during the Cold War, and that MAD might occur today in cyberspace if

deterrence measures were to fail.[22] In his essay, "Cyber Deterrence: Is a Deterrence Model Practical in Cyberspace," Nathaniel Youd again considers the nuclear-cyberwarfare parallel in suggesting that while the threat of MAD may have been the impetus for later attempts at nuclear disarmament, such an event is unlikely with reference to cyberwarfare.[23]

However, applying the literature on nuclear deterrence to the evolving situation in cyberspace is not a perfect fit—for several reasons. In the next section of this Letort Paper, several specific problems, which help to distinguish deterrence in cyberspace from deterrence in the nuclear arena, are considered. These issues include the knowledge problem or the problem of attribution; the temporal problem, or the ways in which time functions in cyberspace as opposed to during nuclear attacks; the payoff or reward structure for both types of events; and the fact that nuclear deterrence was largely an elite activity carried out by specialists, whereas cyber-deterrence is a populist activity that includes several different types of actors and in which publicity, declaratory policy, and signaling become increasingly important throughout the interactions. Table 3 provides a brief summary of these differences in approach.

	Nuclear Deterrence	Cyber-Deterrence
Attribution/ knowledge	• Actors are specified. • Both sides have information about adversary's weapons, strategies, and values.	• Actors are initially unspecified, becoming clearer as the interaction proceeds. • All actors must speculate about others' motives, weapons, strategies, and values.
Temporal frame	• Interactions are not connected. Success in one interaction may not affect capabilities or chance of success in future interactions.	• Interactions are iterated. • As they proceed, both sides acquire more information. • Later interactions may not resemble earlier interactions as strategy, resolve, knowledge, and capabilities evolve.
Payoff structure	• Interaction produces a clear winner and loser. • Action is zero-sum (one side wins while other loses through backing down, or failing to demonstrate resolve).	• Iterated nature means that even the loser gains: He acquires more knowledge about his adversary, which is used against the adversary in a future interaction. • Attacker may gain credibility or fame through launching an attack, even if he fails.
Elite/ populist	• Actions, weapons, and strategies are classified. • Cleared individuals who do not share information carry out actions and strategies. • Public may have a stake in the outcome but does not have any responsibility to participate or be informed.	• Actions, weapons, and strategies may be the subject of public knowledge and speculation. • Individuals, groups, corporations, **and** state actors carry out actions. • Corporate employees and citizens may be called upon to "help" in cyber-deterrence effort through practicing good cyber-hygiene and reporting suspected attacks.
Demonstrate resolve/ capability	• Signaling function may be clear-cut.	• Signaling function is frequently unclear.

Table 3. Differences between Nuclear Deterrence and Cyber-Deterrence.

The Knowledge Problem: Attribution, Puzzles, and Mysteries.

As noted earlier, nuclear deterrence literature relies on a game theory model in which there are clear policy consequences associated with each of the clearly defined choices a state may face. Thus, in describing and understanding how great powers made decisions about how to behave during a nuclear standoff, analysts could assume that they knew who their adversary was, what weapons he or she possessed, the power associated with those weapons and the consequences for each side associated with each policy choice. In addition, the field of nuclear forensics made it possible to identify particular components as belonging to particular actors. In this way, there was a clear trail from the attack back to the attacker.[24] In addition, nuclear deterrence is zero-sum, meaning that in each altercation, one side could be said to have succeeded while the other failed. It was quite obvious in a nuclear standoff who the winner and loser were. Finally, it is obvious what constitutes an act of war in nuclear war: it is the launch of a missile. In contrast, it is not entirely clear what constitutes an act of war in cyberspace, nor are the ideas of territory or boundaries clearly defined or agreed upon within international law.[25]

In addition, as Robert Jervis points out, nuclear deterrence theory suggests that all actors contemplating a nuclear attack see the world in similar ways, based on similar assumptions. Thus, one assumes that they have similar motives and intents as well as a similar time frame.[26] This set of assumptions may well hold in considering nuclear deterrence doctrines, but it is problematic in considering the applicability of these doctrines to cyberspace. Instead, as Robert Siciliano

has noted, cyber-incursions into U.S. Government and private cyber-assets are carried out by a variety of different actors with a variety of different motives. Not all actors see risk the same way, nor are all equally committed to the achievement of their objectives.[27] Indeed, recent discussions about the problem of asymmetric warfare in cyberspace are an acknowledgement of this reality—that deterrence by punishment strategies cannot be "one size fits all"—since not all attackers have the same critical infrastructure and assets belonging to their group or state. Therefore, it is not possible for the United States or another defender to strike back at a group in the same way in which they themselves may have been struck.[28]

However, in thinking about the altercations that have taken place thus far in cyberspace, one is reminded of the words of the analyst Gregory Treverton who drew our attention to the differences between puzzles and mysteries in describing the task of intelligence gatherers today. In his work,[29] Treverton suggests that the task of intelligence during the Cold War was mostly to "fill in the blanks"—or to provide answers to clearly specified questions such as, "How many ICBMs does the Soviet Union have and where are they stationed?" Once one gathered all these puzzle pieces together, one could have a clear picture of the battlefield and the risks associated with various strategies. In contrast, he argues that in the post-Cold War Era, the questions that confront intelligence planners are not puzzles, but mysteries. The questions are frequently broader and less clearly specified. They may include the word "Why" and ask for speculation about motives, which are unclear and sometimes poorly specified. Thus, a mystery might include a query like, "Who are our enemies and why do they wish to harm us?"

We can compare the knowledge environment of the 1962 Cuban Missile Crisis to the Spring 2015 cyber-attacks on the U.S. Office of Personnel Management, believed to have been carried out by the Chinese state-sponsored group Deep Panda. In recent years, Deep Panda has attacked American think tanks and human rights groups, as well as defense, healthcare, government, and technology firms.[30] Here, cyberspace attribution is not a one-time process in which one is immediately right or wrong in terms of one's assessment of who committed the attack. Instead, as Eric Jensen notes, attribution may take place along a spectrum where, "over time a victim becomes more and more certain of who committed the attack."[31] And here, as we can see, intelligence plays a much larger role in helping actors think through and make sense of the battlespace—helping to see through deceptions, such as actors who "spoof" or pretend to be other actors, helping to draw connections between groups who might not at first glance appear to be connected, and providing answers to mysteries such as, "Who is my attacker and what does he want?"

We might also compare the winter 2014-15 attacks on the Anthem healthcare corporation, which are also believed to have been the work of Deep Panda. In the Anthem intrusion, the security firm which investigated the break-in was able to match the Internet Protocol (IP) address associated with the malware to other known IP addresses associated with Chinese government information warfare divisions[32]—but this only occurred after the break-in had been identified. The two parties thus never came "eye to eye"—since the American entity did not immediately realize that they were under attack, nor did they know the identity of their attackers until much later.

The Temporal Problem: The Iterative Nature of Cyber-Defense.

In comparing nuclear and cyber-deterrent environments, one also needs to consider the different temporal environments—or the way in which time factors into decision-making in each environment. Here, as Joseph Nye, Jr. points out, "Nuclear explosions are unambiguous and immediate; cyber-intrusions can plant logic bombs in the infrastructure that may go unnoticed for long periods."[33] That is, the temporal logic for both types of deterrence is different. In the nuclear example, if a defending state wishes to deter an attack through a show of force, that show must take place within a specified period of time in order to cause an attacker to "back down"—as in the Cuban Missile Crisis. Academic writing about nuclear deterrence thus often focuses on situations of high conflict[34] in which both sides adopt "brinksmanship" strategies. The assumption is that there is one particular moment when two adversaries come eye to eye with one another, and in which each side must decide how to react—whether to launch the nuclear weapon or to withdraw.[35]

In contrast, as John Rollins and Clay Wilson note in their analysis of cyberterrorist attacks, cyberattacks are frequently not individual, discrete incidents. Instead, as they point out, cyber-incidents tend to blur the line between war, criminality, and terrorism.[36] Thus, the incidents themselves cannot be neatly defined in terms of either their temporal frame or their effects, which may spill over beyond their original targets. Instead, Rollins and Wilson note that:

Because of interdependencies among infrastructure sectors, a large-scale cyberattack that affected one sector could also have disruptive, unpredictable, and perhaps devastating effects on other sectors, and possibly long-lasting effects to the economy.[37]

Thus, in contrast to nuclear deterrence, cyber-deterrence is not a process that acts during a specified period of time; rather it is a constant and dynamic process, as attackers may come back again and again to attempt to access the same site; they may also retreat from a site and then use information gleaned from the initial assault to re-enter and wreak more damage at a later date. Within cyber-politics, such intrusions are referred to as "advanced persistent threats (APT)." Dmitri Alperovich describes a scenario involving cyberthreats as follows:

The adversaries, especially the nation-state types, don't consider the battle or their mission to be over just because they got kicked out of the network. After all, they have a job to do: get in, and stay in no matter how hard it is or how many roadblocks they face … And till now, the only way to 'win' was to prepare yourself for the long fight with an understanding that the adversaries won't relent and you have to be vigilant and alert to beat back each and every wave of attack.[38]

As the National Nuclear Security Administration notes, the U.S. nuclear security enterprise may experience up to 10 million security events per day, while the U.S. Department of Homeland Security notes that tens of thousands of cyber-intrusions are carried out each year.[39] Thus, Iasiello argues that cybersecurity needs to be both ongoing and dynamic, that while

one's enemy may be temporarily deterred from a particular target, this is seldom the end of the matter.[40]

Furthermore, cyber-deterrence tends to "decay" over time in a way that nuclear deterrence does not, since, as Jensen notes, cyberweapons, unlike nuclear weapons, are "single use" weapons.[41] Once a weapon has been displayed to an adversary and the larger community, its effectiveness is limited. Others can easily copy it and modify it, and the developer seldom has a long-term advantage as the creator of the weapon. As a result, cyber-deterrence strategies are less likely to end in a stalemate, which creates long-term stability — as the nuclear analogy might suggest. Instead, adversaries are likely to experience crisis instability, wishing to act quickly after achieving a new weapon or technology in order to wring all possible advantages out of that situation before it changes once again.

However, the most striking difference between nuclear and cyber-deterrence scenarios is the fact that cyberattacks or cyber-altercations are seldom a "one-off" event that is never repeated. Rather, as Brandon Valeriano and Ryan Maness have shown in their database of cyber-conflict, it is best understood as a set of iterated or repeated interactions, often among the same players who spar again and again in cyberspace. The idea of a stand-off — in the manner of the Cuban Missile Crisis, between two clearly identified and known adversaries — is not the most likely scenario to occur in cyberspace.[42] Instead, Valeriano and Maness suggest that over time, the conflict may heat up, eventually leading to a full-fledged cyberwar, such as what occurred between Russia and Georgia.[43]

The ongoing nature of cyberattack also suggests that since there is no "brinksmanship moment," deterrent strategies are also likely to be less effective in preventing conflict. Within the nuclear arena, we often speak of a brinksmanship crisis, defined by Richard Lebow as "a confrontation in which states challenge important commitments of adversaries in the expectation that the adversaries will back down."[44] That is, classical deterrence theory is concerned not only with preventing enemy incursions once they have been launched or in punishing incursions once they have occurred (or been detected), but also with the notion of "winning through intimidation"—of convincing your enemy that there is no point in attacking you, since he or she would surely lose, and thus causing the enemy to change what he or she wants or chooses to pursue in advance, since there is surely no way to get it. In the nuclear deterrence literature, the notion of MAD assumes that within a clearly defined brinksmanship moment, there are payoffs that both sides would prefer to avoid because their consequences are unthinkable.[45] In this way, the deterrence strategies of both sides can be understood as a way of preventing escalation from a conventional to a nuclear arms race, and on some level, a way of forcing a minimal level of cooperation, which creates collective goods for the community as a whole, including stability (bipolarity) and the absence of nuclear conflict. Nuclear confrontation thus is meant to produce an equilibrium or solution set, which can be reached and will prevent further escalation and create stability. Here we can consider the statement by General Bernard Brodie who stated in 1946: "Thus far the chief purpose of our military establishment has been to win wars. From now on, its chief purpose must be to avert them. It can have almost no other useful purpose."[46]

In considering cyber-deterrent strategies, however, since they lack a brinksmanship moment, it may be preferable to speak of prevention through design, rather than deterrence by denial. The image of multiple actors (individuals and groups) relentlessly hammering against the "gates" of an enterprise to seek entrance seems to have little to do with creating the conditions under which they change their minds about entering — as deterrent strategies would suggest — and more to do with building higher walls, including firewalls, in order to ensure that the target is not overrun. In addition, as noted earlier, would-be intruders seldom abandon their quest; rather they merely move on and choose another target, as is common in prevention through design. As a result, deterrent strategies for cyberspace will need to be long-range targeted, and carried out within an interagency context.[47]

Finally, time behaves differently in cyberspace strategies, since companies today may start with the assumption the hacking has already occurred and the hacker is already inside the network. That is, the "conflict" began without the defender being aware of it. As the defenders respond, they may be said to be "deterring" further actions, but they are clearly not preventing the hackers from entering. Here again, one could argue that what the defender is really doing is more akin to prevention through design, as he builds structures (like mazes, hidden files and decoy files known as "honeypots") to lure attackers away from the assets he or she most wishes to defend.[48] Table 4 shows the timing of event differences between nuclear and cyber-conflicts.

	Nuclear	Cyber
Events	• May be one-off. • Brinksmanship moment.	• May be iterated, ongoing.
Beginning of event	• Declared, obvious—takes place in real time, with real time reactions. • May "win through intimidation" through convincing attacker to back down BEFORE he or she attacks.	• May not be obvious until event has already begun or even finished. • Defender may be reacting to an ongoing event.
End of event	• Obvious: one side backs down and is declared the loser.	• Non-obvious: defender may still not be aware that event has occurred, or may not be able to identify his or her opponent yet.
Properties	• Deterrence can create stability. • Weapons' utility remains relatively constant.	• Weapons' effectiveness decays quickly. • Tendency toward crisis instability, "striking while the iron is hot."

Table 4. Time in Nuclear and Cyber-Conflict.

The fact that conflict is ongoing—often between the same adversaries, occurring along a spectrum where there is no clear end point, beginning point, or brinksmanship moment—has implications for the way we think about the payoffs or rewards that cyberattackers may gain or lose in cyber-conflict today. It also affects how we think about the costs associated with participating in cyber-conflict and in preparing for it.

The Learning Problem: The Payoff of a Failed Attack.

As the previous section has indicated, cyberattacks might be more properly viewed as part of an ongoing campaign, rather than as individual attacks. This

distinction is important, since the reward structure is different for aggressors in a campaign than for aggressors within a specific conflict. The reward structure is also different for defenders in a campaign. In considering cyber-deterrence, two important facts emerge.

First, deterrence in the cyber-realm is not iterative. That is, deterring one attack does not increase your chances at deterring subsequent attacks. Here again, we can distinguish between a nuclear environment in which a player might leverage a success in one interaction into successes in other areas or in future interactions. That is, in the nuclear arena for the United States, prevailing publicly in an event like the 1962 Cuban Missile Crisis created power and credibility that could then be leveraged against future attacks. The United States demonstrated resolve, which made it look more threatening to others within the international system as well as toward the Soviet Union in particular. However, because there is no brinksmanship moment in cyber-conflict today, it is theoretically possible for a defender to beat an opponent's planned attacks and to gain nothing from having done so—because the less public nature of cyber-conflict means there is no guarantee that anyone will know the deterrence occurred. In addition, there is no guarantee that the next attack will resemble the first in any way nor that the next attack will be committed by the same actor.

Secondly, while deterrence is not iterative, cyber-attacks are. That is, while the defender may win little by successfully defending a target, the attacker may win much more—even if he or she does not succeed in obtaining the target, because of the nature of the ongoing campaign being waged. That is, when an adversary succeeds in hacking into a system, the odds are

increased that he or she will subsequently be successful in infiltrating the same or similar systems—since each attack provides more information about the adversary that can be used in preparing subsequent attacks. Succeeding once thus increases the odds that the attacker will succeed again. Thus, paradoxically, a failed attempt in cyberspace might not weaken one's opponent, but might instead strengthen him or her, allowing the attacker to come back later and attempt to attack a target again, equipped with increased knowledge, new skills and perhaps even better outside support. (In contrast, "backing down" from a nuclear confrontation is seen as a failure, which confers no benefit on the would-be aggressor, who may lose prestige within the international community as his or her reputation declines.) This way, even though a cyberattacker may be deterred, he or she may actually be incentivized to wish to return and try a subsequent incursion, armed with the increased knowledge derived from the first attempt.[49] Current strategic thinking about deterrence by denial and deterrence by punishment does not allow for the possibility of one's adversaries deriving a reward within a deterrence scenario, especially when they fail.

This point—about the rewards of failed attempts within the context of an ongoing campaign—can be illustrated through considering the winter 2014 Chinese attacks against Anthem Inc., the U.S. healthcare system. Here, Bill Gertz notes:

> Stolen personal data likely will be used by Chinese intelligence services to identify, locate and recruit potential agents, especially those in the US government or at defense contractors, or for conducting byer attacks against specific high-value targets. . . . By sifting the

stolen Anthem data for records on specific intelligence targets, the Chinese stand to gain a further picture of how to approach these targets.[50]

An article in *Reuters* similarly spoke of a "month-long battle" with the group Deep Panda, also known as Shell Crew, who is believed to have been active since 2011. The author notes that the crew probed the defenses of a U.S. company for 6 months before getting data, which were then used to set up a spearfishing account that company employees fell for, clicking on a link that installed malware. These steps then allowed Deep Panda members to "move freely" along the system for a period of 50 days. The author notes that "for the next 50 days the group moved freely, mapping the network and sending their findings back to base." They then returned 3 months later with specific lists of data they wanted, likely after consulting with other experts.[51] (Cilluffo *et al.* refer to such an attempt as "preparing the battlefield" for a later assault through gathering intelligence.)[52] Indeed, expert Dmitri Alperovich has suggested that China is carrying out a campaign that has included the targeting of state motor vehicle departments and U.S. Investigations Services, Inc. (USIS), a U.S. contractor conducting security clearance investigations.[53] It has been suggested that perhaps all of the attacks may be part of a larger plan aimed at creating a database of prominent Americans.

However, for the defender, it is not always possible to figure out how the attacks are related, and whether an attack is simply a one-off event or part of a larger campaign. (Here we may think again of Treverton's analogy of the mystery versus the puzzle.) In contrast, even in a situation where a would-be attacker

appears to have "lost" by not accessing his or her target, the attacker may have still "won" because of gaining increased knowledge about the target, skills at hacking, and perhaps acquiring an increased reputation within the hacking community based on how successful the incursion was. Thus, the payoffs are asymmetric and biased against the defender.

The Populist Problem: Nuclear Deterrence Is an Elite Activity, While Cyber-Deterrence Is Not.

A final reason the nuclear deterrent example is not a good model for thinking about cyber-deterrence is the difference between the elite, specialized, and classified nature of nuclear deterrence activities and the more populist and public nature of cyber-deterrence activities. While one can speak of "public moments" in nuclear deterrence, such as the Cuban Missile Crisis, for the most part, nuclear deterrence has been a highly specialized, elite activity. Those who work daily with missiles are largely military personnel or contractors holding high-level security clearances. Little public attention is paid to their activities or to them.

In contrast, cyber-deterrence today may require cooperation by all users of a technology. Just as U.S. security officials have enlisted the cooperation of American citizens in being vigilant against terrorism, campaigns have also asked Americans to pay attention to their cybersecurity—from safeguarding their personal information, to choosing good passwords and being careful not to respond to phishing attempts. The problem is that while deterrence for defensive purposes appears to require the cooperation of all users, attacks do not. Instead, they may be carried out by groups like Deep Panda without citizens on either side being aware of them.

III. WHY BORDER DETERRENCE THINKING IS MORE APPLICABLE THAN NUCLEAR DETERRENCE THINKING

As the previous examples have shown, the nuclear example is not an exact fit for those who wish to "borrow" deterrence strategies and apply them in cyberspace. Differences in the temporal frame, the reward structure, and the elite versus populist strategies used suggest that applying the nuclear analogy may be more confusing than helpful. In contrast, as I have argued in Section I, a better example may be drawn from the literature not on nuclear deterrence but on criminal deterrence. In particular, the best way to think about how to deter would-be aggressors in cyberspace may be to borrow key tools and lessons from the efforts of U.S. border security forces, which have attempted to defend U.S. borders from authorized real attacks in real space.

There are several reasons the border security analogy more neatly tracks with the cyber-incursion situation. First, both types of borders are porous and difficult to guard. As Kelly Gable has written, the main threats that exist in cyberspace come about because of inherent weaknesses, which are built into the structure of cyberspace and its technologies. Namely, it is leaky or porous; has poor borders, which are not well defined and are nearly impossible to police. She writes:

> The primary security threat posed by the internet is caused by an inherent weakness in the TCP-IP protocol, which is the technology underlying the structure of the internet and other similar networks. This underlying structure enables cyberterrorists to hack into one system and use it as a springboard for jumping onto any other network that is also based on the TCP-IP protocol.[54]

Clorinda Trujillo notes that a number of issues complicate the problem of how best to guard cyberspace. The fact is, that the assets that make up cyberspace may be comprised of infrastructure and data belonging both to the government and to corporations. In addition, the "borders" of cyberspace may be unclear, since assets belonging to one country (like data) in reality may be housed in another country (which may maintain and house the servers).[55] Nonetheless, since 2006, the U.S. Department of Defense has maintained a posture that would deny entrance to potential aggressors who attempt to achieve objectives in U.S. cyberspace. As noted in the 2006 *Quadrennial Defense Review*, the U.S. posture serves both to deter those who would seek entrance to U.S. cyberspace, as well as to persuade would-be interlopers not to make the effort, as they are likely to fail.[56] This way, the U.S. military could be said to have already spent nearly 10 years attempting to guard its borders in cyberspace. Thus, it is possible to compare and contrast the efforts of U.S. border patrols in both real space and cyberspace during that period.

1. A Variety of Actors Involved in Creating and Enforcing Deterrent Strategies.

We can also draw parallels between the variety of actors involved in deterring border crossings in the real and virtual worlds. In both cases, conflicts are created between a variety of different state actors on the federal, state, and local levels. Although the responsibility for policing borders lies formally with the federal Immigration and Customs Enforcement (ICE) agency, in reality the responsibility for identifying those who

have breached our borders may fall on state troopers, local police, and even social services agencies acting in a border area. Illegal immigration costs all of these organizations money, and it is in the interests of all to cooperate in implementing policies, which are drawn on the federal level. Yet, in reality, with the problem of sanctuary cities, all of these organizations may not be on the same page in terms of border security. All may not agree about the threat played by territorial incursions or be willing to commit their resources to address the problem. Some actors, like corporations, may even benefit from illegal immigrant labor and thus have no vested interest in committing resources to combat the problem.[57] Moreover, as with cybersecurity, the responsibility for coordinating the disparate responses and for making policy is at the federal level. That is, both in virtual and in real border security, the lead is taken by the federal government, with additional responsibilities being parceled out to other actors at state and even local levels, including appropriate civilian and business authorities.[58]

Similarly, with incursions into cyberspace, U.S. Cyber Command, under U.S. Strategic Command, is responsible for defending Department of Defense computer systems and conducting full-spectrum military cyberspace operations.[59] However, as Trujillo points out, U.S. Cyber Command does not work alone in defending American cyberspace. Instead, as she notes, the 2002 U.S. *National Security Strategy* speaks of a requirement to detect and deter international espionage efforts, which might involve using cyber-capabilities. The main responsibility for combatting such attempts is given not to the U.S. military, but to those government agencies involved in enforcing trade agreements—including the Department of Com-

merce and the Department of Justice.[60] This way, both military and civilian agencies (including commercial entities) and employees are asked to work together in protecting the "borders" of cyberspace.

In both situations, there is a primary player (U.S. Customs and U.S. Border Enforcement, or U.S. Cyber Command), which is also backstopped by a number of players with related missions. As Wayne Cornelius and Idean Salehyan point out, the deterrence mechanisms placed around our nation's borders are multi-layered, including ships, planes, advanced radar, and personnel.[61]

Lesson One: Both problems—deterring real and virtual border crossings—require a complex set of deterrence solutions.

These solutions must be choreographed by a wide variety of actors, not all of whom are equally committed to allocating resources or solving the problem.

- In both cases, it is thus important to designate a single point of contact who is responsible for coordinating diverse efforts as well as exploring what might be required to get "buy-in" from all key actors. Thus, we have seen the appointment of a Policy Czar for Illegal Immigration as well as a Special Assistant to the President and Cybersecurity Coordinator.[62]
- In both cases, it is also important to define terms and to make sure that all players share understandings, as well as to define clearly the sphere of responsibility. Defining terms and spheres of responsibility is likely to be a point of contention in both cases.

2. A Variety of Different Types of Trespassers.

Next, in considering the "knowledge problem," the border incursion scenario more closely resembles the cyber-situation than the nuclear scenario does. At any given time, U.S. border control agencies must be prepared to fend off an unknown and somewhat unpredictable number of possible trespassers in a poorly defined information environment. Those who seek to access America's physical borders may include men, women, and children; they could be career criminals, starving refugees, or possible terrorists. The skills, tools, and motives of the trespassers vary by status and occupation and therefore, the same strategy for preventing access may not work for each group.

Similarly, cyber-analysts have identified seven different types of "hackers" or intruders, including:
- Tool kits or newbies who may follow instructions found on bulletin boards to carry out simple computer exploits;
- Cyberpunks, who may be interested in activities such as defacing web pages, often for political or ideological reasons;
- Internals, who may be disgruntled employees working within an existing company's computer department;
- Coders;
- Old Guard hackers, who may be interested in the intellectual challenge of accessing a computer system;
- Professional criminals; and
- Cyberterrorists.[63]

Siciliano offers a slightly different typology of possible hackers and their motives, which are summarized as:

- White Hat Hackers, who may wish to test their own company or other company's systems in the hopes of identifying weaknesses they will then report to the companies;
- Black Hat Hackers, who usually work for money, hacking into systems illegally;
- Script Kiddies, who usually seek fame for their exploits, often using borrowed programs;
- Hacktivists, who are often motivated by politics or religion;
- State-Sponsored Hackers;
- Spy hackers, who may be hired by corporations and may sometimes act as moles, working in corporations to get access; and,
- Cyberterrorists.[64]

Cilluffo *et al*. also point to a variety of types of adversaries, which the United States (or any nation) may face in cyberspace—including foreign militaries, foreign intelligence and security services, nonstate terrorist organizations, nonstate criminal enterprises, and hybrid aspects (such as one actor acting as a proxy for another).[65]

The lesson here is clear: Both in real space and in cyberspace, border crossing is an activity practiced by different types of people with varying levels of commitment to achieving their target. Some are ranked as amateurs, while some are professionals. Some are primarily motivated by benign reasons, while others are not. Some percentages in each group are terrorists. As John Mowchan points out in reference to the cyber-problem:

> Non-state actors include hackers, hacktivists, terror-
> ists and organized crime groups. Hackers are thrill-
> seeking individuals. . . . while hacktivists use cyber-
> space to protest or promote their political beliefs. Both
> usually don't possess the technical skills to attack ef-
> fectively government networks; however, state actors,
> seeking to avoid attribution, could provide them with
> the necessary tools to degrade or damage U.S. govern-
> ment networks.[66]

In each case, planners need to design different de-
terrence strategies for different groups who may have
different motivations and different levels of commit-
ment to achieve their objectives. Unfortunately, as
Scott Helfstein *et al.* point out in their study of nuclear
terrorists, a paradox exists: Those who are most like-
ly to be deterred from their objectives by a show of
force on behalf of the defender are probably the least
dangerous and least committed intruders. In contrast,
those who are least likely to be deterred are likely to
be well-resourced (possibly state-sponsored); they
may also have a higher level of ideological commit-
ment to the achievement of their objectives. Indeed,
it is possible that those that are strongly ideologically
committed to an action will be incapable of being de-
terred—since their motivations are fundamentally
less rational.[67]

Douglas Tippett again argues in favor of a targeted
deterrence strategy, noting that a deterrent strategy is
seen as less credible if retaliatory threats are not ap-
propriate to the actions being threatened. Although he
is speaking about our U.S. anti-terrorism strategy, his
point still holds. He argues that "policy threats lack
credibility because the signaled response to terrorism
holds constant across varying degrees of attack sever-
ity."[68] He suggests that those who consider and plan

attacks are rational actors who think through the possible costs and benefits, as well as the risks. If, however, we accept that there are different types of actors making these calculations, we might also conclude that they will not all arrive at the same answer or use the same calculus in thinking about risk.

The Threat Resides Both Outside and Within our Borders.

In addition, both those concerned with border security and those concerned with virtual security must consider not only those who wish to access the system but also those who are already in the system. For both in real space and virtual space, trespassers have the ability to reside within the system undetected for a long period of time. Accounts of the December 2014 Sony hack point to the fact that a number of attempts were made by the hackers to trespass into the system. Hackers did not simply visit the site once but also "moved in," succeeding in mapping out drives and becoming familiar with the contents of the servers before deciding how best to attack them and what to release. Paul Roberts refers to "low and slow" attacks, in which people evaded notice and were in the system for a long time; he suggests that both the attack against Saudi Aramco and Sony fit this pattern.[69]

In addition, in both border security and cybersecurity situations, "insiders" who are already within the system and who may possess information and intelligence, which can be shared with would-be intruders in order to increase their efficacy and chances of success, may aid those who seek to access the system. Analyses of the cyberattacks on Russia's banking sector, which took place between 2013 and 2015, point to the fact that the employees within the organiza-

tions targeted most often provide the "way in" to the targeted systems.[70] Employees may unknowingly assist those attempting to access their systems through downloading malware onto their own computers as a result of opening e-mails and files, or they may consciously agree to work with hackers attempting to access a system.

Thus, it is obvious that in both situations, it is important to consider the whole process or life cycle of incursions. In describing how hackers can come to own a system, analysts often refer to the so-called "cyber-exploitation life cycle." The cycle includes eight steps:

- Initial reconnaissance (which includes both target selection and target research, or "profiling" one's target);
- Penetration;
- Gaining a foothold;
- Appropriating privileges;
- Internal reconnaissance;
- Maintaining presence;
- Exfiltration; and,
- Accomplishment of the mission.

Dimitar Kostadinov thus describes cyber-exploitation as "an evolving occurrence which . . . has an inception, development, main activity/culmination, outcome, and eventually consequences." [71]

In considering deterrence strategies then, we should differentiate strategies depending on the nature of the attacker and the point in the life cycle at which activities are occurring. Just as the majority of those who seek to enter the United States illegally do not ultimately wish to harm the United States, some individuals who hack into computer systems illegally may not have malicious motives in doing

so. The same deterrent strategies will not work for all subgroups of "trespassers"; it is thus imperative for those designing deterrent strategies to figure out whom they wish to deter, and then to design strategies aimed at those groups in particular. Here again, a lesson may be drawn from U.S. immigration policy and law in recent years. Particularly under the Obama administration, the decision has been not to "waste resources" on people who are not "real criminals." Thus, the bulk of resources devoted toward combatting illegal immigration have been devoted to prosecuting and pursuing career criminals and those who are more likely to harm the United States through actions such as terrorism. At the same time, the United States has identified a low level of illegal immigration, which it is willing to accept without devoting resources to pursuance and prosecution.

Lesson Two: We Need Targeted Strategies Against Intruders.

- In developing a deterrence strategy for preventing cyber-intrusions, it is important for planners to decide whom we most want to deter and develop a nuanced response in terms of deterrence by design, by denial, and by punishment.
- Leaders need to commit resources to stopping attacks at all stages of the attack cycle, including taking deterrent measures against those already within the system.

3. We Have No Strong Norms Against Incursions.

Perhaps the most striking parallel with illegal immigration is the fact that in both cases, the U.S. Government has been unsuccessful in establishing a norm that would lead would-be intruders to change their preferences regarding the practice. (In contrast, Nye argues that there is a strong norm established against the use of nuclear weapons.[72]) Instead, as Cornelius and Salehyan note, in the period since the early-1990s, the U.S. Government has quadrupled its spending on border security, but has not experienced a quadrupling of its success in deterring illegal immigration. Instead, they point out, it simply costs more today to capture a would-be immigrant than it did in the 1990s—since the hiring of agents has roughly kept pace with the number of immigrants who now attempt to cross the borders. However, the overall percentage of those apprehended has stayed relatively constant.

As a result, in both immigration and cyber-literature, analysts argue for the necessity of defining a low level of intrusion, which is seen as inevitable and acceptable though undesirable. They also argue for the necessity of defining a "red line" or level of intrusions, which would be regarded as unacceptable and therefore would receive some form of retaliation. In both cases, there is an understanding that no method of deterrence will be 100-percent effective. Presidential Policy Directive-20 (PPD-20) also acknowledges this problem, noting that:

> The United States recognizes that network defense, design, and management cannot mitigate all possible malicious cyber activity and reserves the right, consistent with applicable law, to protect itself from malicious cyber activity that threatens U.S. national interests.[73]

41

As a result, both in cyber-deterrence and border security, officials have begun to distinguish between the types of intruders who are most likely to make attempts—creating targeted deterrence strategies, depending on the character of the intruder. However, the decision of illegal immigration or to accept some low level of cyber-intrusion is problematic, because it may suggest in some way that these activities that occur below that level are in actuality regarded as legitimate or acceptable. Helfstein *et al*. made the same argument in describing the various types of terrorist threats that the United States may face and the different strategies that might therefore be required. Here, they argue that "by establishing a specific red line, a state runs the risk of legitimizing the more moderate but still lethal kind of terrorism to some degree."[74]

Lesson Three: Accept the Impossibility of Establishing a Norm Against Cyber-Intrusion.

Planners may wish to consider accepting some low level of intrusions by those who are merely annoying and not harmful.

4. We Are Fighting a Long War Against Illegal Immigration and Cyber-Incursions.

Next, the attempts by border authorities to preempt, prevent, and respond to border incursions have the character of a campaign or "long war," similar to the campaigns of the U.S. Cyber Command today. Over time, combatting illegal immigration can lead a nation to exhaust itself economically and in terms of manpower. Combatting illegal immigration also has a constant opportunity cost, because funds must be

spent on border security rather than on other community needs, such as the need for education or social services.

Similarly, within the area of cyber-defense, Amir Lupovici refers to a strategy of "serial deterrence." He argues that "Cyber-attacks are very likely to turn out to be manageable primarily through applications of serial deterrence, repeated harmful responses over an extended period, to induce either temporary or eventually permanent suspensions of the most bothersome attacks or attacks by the most obnoxious opponents."[75] As it relates to continual or serial deterrence against illegal immigration, the strategy rests on an acknowledgement that the "enemy" will not be completely defeated, although police organizations may seek to infiltrate and destroy criminal elements associated with people smuggling and human trafficking.

It is also important to recognize that in both the immigration and the cyber examples, targets are often not fungible. In other words, if would-be immigrants are unable to enter the United States along its southern border, it is doubtful that they would merely choose to enter another country instead. Similarly, it is unlikely that would-be entrants into American cyberspace could be redeployed to other targets elsewhere. Thus, if intruders are stopped at one entrance, they will not abandon their quest for entry but will instead choose other less well-guarded targets. They will also not make a one-time attempt at each entrance, but rather will return persistently, seeking new weaknesses and points of entry, and new means of deception (such as false papers or identifications, etc.)

In both the cases of illegal immigration and attempted cyber-incursions, it becomes clear that attempts at incursion are both ongoing and periodic. That is, the number of attacks are not constant over time but rather occur in somewhat regular waves and cycles, in response to specific events. In the case of illegal border crossings and illegal immigration, one can identify scenarios in which a short-term vulnerability is identified, such as an unguarded outpost or a new method of smuggling. In such a situation, one can expect to see a wave of attempts until the receiving country identifies the vulnerability and closes it.

Similarly, cycles of cyber-conflict may arguably be both predictable and predicted. Cyberattacks may increase in number and intensity due to other events occurring between rivals at the time, in which cyberattacks are merely part of the strategy utilized (i.e., Increases in cyberattacks between Russia and Georgia combined with conventional fighting between rivals).[76] They may also increase as a result of crisis instability. The understanding is that a player may wish to exploit a short-term advantage he or she has over opponents and thus may be driven to launch an attack before the window of vulnerability against those opponents is closed. A case study of the Anunak cyber-hacker group in Russia notes a similar "wave" of attacks on the Russian banking sector. A new wave of cyberweapons to be used for cyber-incursions was developed, which was then used in a heavy series of attacks throughout late-2014 until Russia's banks became aware of the problem and sought to close the security hole.[77]

Lesson Four: Understand the Mindset of the Attacker and the Nature of His Campaign.

- Accept that those who seek to enter cyberspace are committed to this action. They will wage a "campaign," making multiple attempts to enter the space.
- One set of barriers will be insufficient to counter intruders, and no set of barriers or set of punishments will be sufficient to establish a norm against trespassing or to change the calculus of those contemplating action against the border significantly. In short, the target is too valuable and too desirable for the would-be intruders simply to abandon attempts to access it.
- Accept that the United States and American assets—both governmental and commercial—will always be the target of cyberattacks.

5. The (In)Effectiveness of Using Publicity to Communicate One's Commitment to Deterrence.

It is widely acknowledged that a successful deterrence strategy often rests on the ability of the defender to communicate a policy clearly and explicitly to those whom it is intended to deter. To that end, some cyber-analysts have even voiced support for a policy in which the United States would exercise great transparency in publicizing the capabilities of units such as the U.S. Cyber Command. As Lupovici argues, such a policy could help communicate U.S. resolve to defend cyberspace. Toward that end, he even suggests revealing budgets, resources, and manpower dedicated to the subject—to increase the credibility of the deterrent message.[78]

However, in their study of Operation GATEKEEP-ER, an initiative launched in October 1994 under the Clinton administration to deter illegal immigration in the San Diego area, Cornelius and Salehyan found that high-profile efforts at raising the perceived costs of illegal immigration do not always have the intended effect. Operation GATEKEEPER included an increase in the number of border patrol agents deployed, the number of hours during which watch patrols were deployed, and in the numbers of apprehensions made. This very public strategy was meant to increase the visibility of border agents and cause would-be immigrants to reconsider the costs attached to their quest and their likelihood of failure. The plan included the construction of 70 miles of fencing along the border, along with the addition of remote surveillance systems, infrared monitors, seismic sensors that detect footsteps, helicopters, and unmanned aerial vehicles. At the same time, a database was constructed to track repeat entrants and people smugglers.

The authors note the immigrants interviewed perceived that it was now much more difficult to cross the borders, as well as more dangerous. Over half were able to name someone who had died as a result of an attempted crossing. However, the authors still brand the deterrence attempt as a failure. Operation GATEKEEPER and the earlier Operation HOLD THE LINE in El Paso, Texas, were meant to preempt immigration attempts and not simply to capture more would-be immigrants. The U.S. Government believed that would-be immigrants could be dissuaded from **attempting** a crossing if they understood from the beginning that they were likely to fail at their attempts.

However, the authors suggest that Operation GATEKEEPER did not have the intended effects. In particular, it appears that Operation GATEKEEPER may have been effective in deterring "amateur immigrants" from attempting a border crossing, but that it was less effective in deterring professionals, including those involved in organized crime and human trafficking. As a result, they suggest, many more families were simply driven into the arms of human traffickers, whose expertise they now relied on in a more risky and dangerous immigration environment. Smugglers meanwhile saw an increase in their business, along with the ability to charge higher fees for their services.[79]

Similarly, Clement Guitton questions whether high-profile attempts to "go after" hackers will be successful. He notes that while publicizing a campaign of increased penalties and enforcement may have the effect of reducing the number of attacks on systems by 35 percent, at least in the short term, many companies do not want to participate in such publicity campaigns because they fear the effects on their investors after admitting that their companies have been the targets of hackers.[80] In addition, raising the legal penalties, including fines and jail time, for those caught attempting to hack in, might discourage those hackers who are largely hobbyists, but such disincentives might not have the same effect on those who are hacking on behalf of foreign governments, including foreign militaries and intelligence operations.

Another striking parallel between the immigration and cyber-examples is the fact that in both cases there is a fair amount of confusion and misunderstanding regarding the legislation that currently seeks to regulate and punish unauthorized intrusions—either

because legislation does not exist for all situations or because all players are not clear what the legislative rules are. In both the cyber and immigration examples, it is unclear under whose jurisdiction the intrusions should be prosecuted. In the case of cyber-intrusions, disputes have centered around whether attackers who were found responsible should be tried in the country where they themselves were located while carrying out the violation, in the state from which the attack emanated (which might be a third party through which traffic is being routed), or in the country where the damage was actually inflicted—for example, upon a computer located on Wall Street in New York. Thus, it may be unclear what criminal penalties may apply.[81]

In addition, as Guitton points out, it is more difficult to deter an attack when hackers themselves may be unclear regarding the legality of their actions. They may not know that their trespass is illegal (or may claim not to know). He notes that "deterrence occurs when a potential offender refrains from or curtails criminal activity because he or she perceives some threat of a legal punishment for contrary behavior or fears that punishment." Therefore, the threat of punishment raises the potential attacker's perception of the costs of such conduct.[82] However, attackers may not fear punishment if they do not realize that these actions are illegal. Similarly, in the spring and summer of 2014, many families sent their unaccompanied children to the United States illegally because they misunderstood the terms of the amnesty that President Obama had offered to U.S. children who had been in the United States illegally for a longer period of time. They sent their children to the United States, believing that it was legal to do so.[83] Here again, efforts at deterring such actions failed, largely because the signaling

message was not clearly communicated to its target nor understood.

In both cases, the United States is also constrained because of its own commitments to uphold the U.S. Constitution and respect the rule of law, even when intruders do not. In combatting illegal immigration, the United States is to some degree constrained by its own laws and policies—including rules that allow for the granting of citizenship to illegal children born within our borders as well as the need to provide illegal citizens with healthcare, education, and other services and rights. Similarly, Paul Rosenzweig argues that U.S. deterrence efforts are weakened due to the requirement that the United States combat cyberattacks within the bounds of its own Constitution and rules.

Lesson Five: Consider How Best to Communicate Deterrent Policies but Recognize the Limitations on Doing So.

- Consider that some audiences will be more receptive to a deterrent message than others. Consider who will be deterred as a result.
- Consider the costs of transparency and whether the risks of transparency outweigh the reward of deterring potential attackers.
- Work with all partners to develop clear penalties for would-be intruders and to resolve issues of jurisdiction.

6. The Problem of Asymmetric Payoffs: Intruders Have Little Incentive Not to Try Again.

Like the cyber-deterrence problem, the border incursion problem rests on a system of uneven rewards. In both situations, those who seek to trespass or access a system are often multiple offenders who learn something each time they make an attempt, whether or not they are successful. An attempt thus costs little while promising a reward with either success or failure. The penalty for would-be immigrants who are caught is usually a bus ride to the U.S. border, from which they may again commence attempts to access the United States. It is thus not surprising that in both situations, individuals make multiple access attempts. The reward system is thus asymmetric between intruders and those who seek to defend a space.[84]

Thus, as Espenshade points out based on his study of undocumented immigrants in the United States, when a would-be immigrant may be unsuccessful at traversing a border at one point, he or she will seldom abandon those efforts. Instead, the would-be immigrant will simply change tactics and targets.[85] Thus, the would-be immigrant might, for example, "up the ante" by hiring a professional coyote to assist him or herself and family with the border crossing if he or she is unable to carry out these plans independently. Here, we can draw a parallel between the foreign government and corporation that outsources hacking through purchasing the services of mercenary hackers. Espenshade notes that:

> Among questionnaires administered. . . . The number of attempts was always one greater than the number of apprehensions; That is, all migrants simply tried until

they succeeded. Apprehended or not, every migrant who attempted to enter the US eventually got in.[86]

Espenshade notes as well that the would-be immigrant might also choose a different point at which to attempt a border crossing—for example, to flee through a rural desert area rather than along a main route.

In the language of deterrence, the choice to find a different path for achieving a target is referred to as "designing around" a particular state's deterrence policies.[87] One can quote Thomas Schelling's finding that "if deterrence fails it is usually because someone thought he saw an 'option' that the American government had failed to dispose of, that it hadn't closed."[88]

In both the border security and the computer security scenario, one can thus see that deterrence strategies often fail because, as Jervis notes,[89] a state often tries to deter others from taking specific actions rather than attempting to deter all actions aimed at a specific objective. As a result, the state's opponent can figure out how to "go around" barriers to realize the objective. Case studies in criminology often reveal a failure of imagination on the part of would-be deterrers. They simply cannot think of all the possible ways open to the other person to change the status quo—even ways that in retrospect seem obvious.

As Sarah Bohn and Todd Pugatch argue, states that engage in large-scale deterrence initiatives, such as hiring an extra 1,000 police officers to engage in border patrol activities, may end up simply transferring the problem to their neighboring states, who become the new targets. That is, deterrence strategies may make sense for one locality, but they do not eliminate the problem—they simply transfer it to a new location.[90]

Thus, any attempt to deter incursions at one point along America's borders may succeed in the short run, but it will not fundamentally solve the problem of ending illegal immigration, since it is impossible for the United States to devote the same amount of resources to watching every point along America's borders with the same degree of scrutiny.

Lesson Six: Understand the Mindset of Attackers, Including How They Think About Reward and Risk.

- Know that attackers may work together in formal or informal coalitions to share information about weaknesses, and undefended borders.
- Realize that if intruders are "deported" or kicked out of the system, they will not merely return home, but will instead attempt re-entry. Some will succeed in gaining entry but will not immediately reveal themselves as intruders. Instead, they may seek to assimilate or hide within the system, in some cases behaving as legal entrants for a period of time. (In the case of cyber-intruders, they later reveal zero-day exploits.)
- Consider how to establish mechanisms that would penalize would-be intruders—and their "sponsors"—for failed attempts, thereby raising the costs of an attempt. How much might U.S. defensive measures cost to would-be intruders—either in terms of damage to their physical equipment or their professional reputations? Perhaps the United States could establish a database of cybercriminals and implement penalties such as denying student visas (or all visas) to suspected cybercriminals. Could the

judicial system treat trafficking in code similarly to drug trafficking? Perhaps credentialing agencies, which vouch for a computer expert's knowledge and skills, could "disbar" suspected cybercriminals in the same way that physicians or lawyers could lose their licenses for unethical behavior. Could an attempt to enter a system be met with some form of physical response, which would destroy the hacker's equipment, costing him resources and time? There are opportunities here if we are able think creatively!

7. We Need a Strategy and Not Merely a Set of Tactics.

The final lesson for cyber-deterrence that we can derive from an analysis of border deterrence is that what is needed is a long-range, nuanced strategy—which takes into account the causes of the problem, the motives of the sponsoring country and the economic and political factors that act in concert with the specific problem. That is, what is needed—both in the cyber-realm and in the actual border security realm—is not merely a set of tactics to respond to particular incursions. As Cilluffo *et al*. have noted, planners need to fight the tendency to craft a deterrent or defense strategy that is incident-driven or ad hoc, marshalling resources only to respond to particular incursions without considering the big picture.[91]

Those who study border security speak of two types of factors that create illegal immigration: Push factors refer to events or incidents in the sending country, which make it an undesirable place; while pull factors refer to the factors that make the United

States so attractive a target for would-be immigrants. This paradigm acknowledges the reality that those who seek to evade border security do not come from nowhere and that in many instances the sending country may be complicit in producing the stream of illegal immigrants. Thus, a strategy for reducing the problem would hold the sending country responsible, as well as working cooperatively with that country to reduce the factors that produce the immigrant stream. In some instances, when a nation is felt to be complicit in allowing illegal immigration to a neighboring country, it may be necessary for the receiving country to sanction or punish the sending country until it takes responsibility for the problem.

The border security literature is also helpful in suggesting that illegal immigration might be thought of as a symptom, rather than the problem itself.[92] In particular, the need for individuals to traverse borders to secure gainful employment suggests a market failure, since employees are not available in the locations where they are needed, and jobs are not available in other regions. Again, what is needed is a comprehensive, international, long-term strategy for addressing that market failure or overabundance of employees in one region. A truly comprehensive strategy for deterring illegal immigration to the United States would necessitate a working relationship between the U.S. and Mexican governments to provide economic opportunities for Mexican citizens within Mexico itself, as well as pressuring the Mexican government to provide better healthcare and education and fewer human rights abuses.

Similarly, a comprehensive cyber-deterrence strategy would necessitate identifying the nations that are likely producers of the majority of cyberattackers, and

it would require that the U.S. Government sit down with its counterparts to consider the motivations of cyberattackers as well as the complicity of the sending state. Here, sticks and carrots could be used to forge a more cooperative relationship with the sending nation. That is, one could also rely on the proposed cyber-strategy of "entanglement" to create structures in which both the target and the producer of the cyberattack are affected by the damages that have been created and in which both have an incentive to cooperate so as to not produce further attacks.[93]

Lesson Seven: Recognize That Cyberattacks Do Not Arise in Isolation and Cannot Be Solved in Isolation.

Work to develop deterrent strategies that take this perspective into account.
- Recognize that cybersecurity, like immigration, needs to be addressed as part of a broader conglomeration of issues. As Rosenzweig has noted, cybersecurity should not be addressed only on a military level through military-to-military actions; it needs to be considered within a broader constellation of national and international issues (including economic competitiveness, etc.).[94]
- Recognize as well the importance and flexibility provided through a policy that allows the United States to respond to cyberattacks not only with cyberweapons but also with other means—such as economic or political ones. This policy is referenced in the 2011 U.S. *International Strategy for Cyberspace*.[95]

CONCLUSIONS

As this Letort Paper has shown, it is too simplistic to merely map the existing nuclear deterrence literature in talking about deterrence in cyberspace. Cyberspace has many unique facets, as does cyber-conflict, that do not exactly line up with the issues, assumptions, and strategies utilized by those engaged in nuclear conflicts. Indeed, it may be that there are other analogies—such as the immigration analogy—that provide a better fit for thinking through the best strategies for deterring cyber-incursions. The immigration analogy is particularly useful for exploring how would-be intruders learn, how they think about the costs and benefits of launching an incursion, and how they would work together to share and draw up informed strategies. As noted, this analogy also helps those seeking to defend a border or target to understand the importance of working together so that targets are effectively shut down rather than merely shifted. Finally, this analogy is important in considering the long-term nature of cyber-defense and the ways in which one must address the underlying structural factors, which both create the problem and, hopefully, contain its solution.

ENDNOTES

1. See Alexander Wagenaar *et al.*, "General deterrence effects of U.S. statutory DUI fine and jail penalties: Long-term follow-up in 32 states," *Accident Analysis and Prevention*, Vol. 39, No. 5, 2007, pp. 982-994.

2. See Lynn Zimmer, "Proactive Policing Against Street-Level Drug Trafficking," *American Journal of Police*, Vol. 9, No. 1, 1990, pp. 43-74.

3. Anthony M. Pate and Edwin E. Hamilton, "Formal and Informal Deterrents to Domestic Violence: The Dade County Spouse Assault Experiment," *American Sociological Review,* Vol. 57, No. 5, October 1992, pp. 691-697.

4. Zimmer, pp. 43-74.

5. This point about the ways cyberattacks threaten to disrupt the stability of cyberspace is made in Stephan Haggard and Jon Lindsay, "North Korea and the Sony Hack: Exporting Instability through Cyberspace," *East-West Center Asia Pacific Issues*, No. 117, May 2015.

6. Frank J. Cilluffo, Sharon Cardash, and George Salmoiraghi, "A Blueprint for Cyber Deterrence: Building Stability Through Strength," *Military and Strategic Affairs*, Vol. 4, No. 3, 2012, p. 6.

7. Wagenaar *et al*.

8. C.R. Jeffery, *Crime Prevention Through Environmental Design*, Thousand Oaks, CA: Sage Publications Inc., 1977, p. 351.

9. Emilio Iasiello, "Is Cyber Deterrence an Illusory Course of Action?" *Journal of Strategic Security,* Vol. 7, No. 1, Spring 2014, pp. 54-67.

10. Chaim Braun and Christopher F. Chyba, "Proliferation Rings: New Challenges to the Nuclear Nonproliferation Regime," *International Security*, Vol. 29, No. 2, Fall 2004.

11. Sean Barnum, *Standardizing Cyber Threat Intelligence information with the Structured Threat Information eXpression (STIX)*, Washington, DC: MITRE Corporation, 2014.

12. My thinking here is based on my reading of Barnum.

13. Amitai Etzioni, *The Hard Way to Peace: a New Strategy,* New York: Crowell-Collier Press, 1962.

14. Henry Wechsler, Jae Eun Lee, Toben F. Nelson, and Mei-chun Kuo, "Underage College Students' Drinking Behavior, Access to Alcohol, and the Influence of Deterrence Policies: Findings from the Harvard School of Public Health College Alcohol Study," *Journal of American College Health*, Vol. 50, No. 5, 2002.

15. See Chad C. Haddal, *Congressional Research Service Report for Congress: People Crossing Borders: An Analysis of U. S. Border Protection Policies*, Washington, DC: U.S. Library of Congress, Congressional Research Service, 2010.

16. My thinking here is actually affected by my earlier work on deterring property squatters in urban areas, particularly the chapter on The Netherlands' revision of its property laws. See Mary Manjikian, *Securitization of Property Squatting in Europe*, New York: Routledge, 2015, pp. 157-174.

17. Michael Newton and Larry May, *Proportionality in International Law*, Oxford, UK: Oxford University Press, 2014.

18. See Daniel S. Nagin and Greg Pogarsky, "Integrating Celerity, Impulsivity and Extralegal Sanction Threats into a Model of General Deterrence: Theory and Evidence," *Criminology,* Vol. 39, No. 4, 2001, pp. 865- 892.

19. See, for example, Joseph S. Nye, Jr., "Nuclear Lessons for Cybersecurity?" *Strategic Studies Quarterly*, Winter 2011.

20. See Dorothy E. Denning, "Rethinking the Cyber Domain and Deterrence," *Joint Forces Quarterly*, 2nd qtr. 2015, available from *ndupress.ndu.edu/Media/News/NewsArticleView/tabid/7849/ Article/581864/jfq-77-rethinking-the-cyber-domain-and-deterrence. aspx*, accessed August 11, 2015.

21. See, for example, Kenneth Geers, "The Challenge of Cyber-attack Deterrence," *Computer Law and Security Review*, Vol. 26, No. 3, 2010, pp. 298-303.

22. Geers, p. 302; See also Matthew D. Crosston, "World Gone Cyber M.A.D.: How Mutually Assured Debilitation is the Best Hope for Cyber Deterrence," *Strategic Studies Quarterly*, Spring 2011, pp. 100-116.

23. See Nathaniel Youd, "Cyber Deterrence: Is a Deterrence Model Practical in Cyberspace?" *Space and Defense*, 2015.

24. Denning.

25. Jeffrey L. Caton, *Distinguishing Acts of War in Cyberspace: Assessment Criteria, Policy Considerations, and Response Implications*, Carlisle: Strategic Studies Institute and U.S. Army War College Press, 2014.

26. Robert Jervis, "Deterrence Theory Revisited," *World Politics*, Vol. 31, No. 1, October 1978, p. 296.

27. Robert Siciliano, "Seven Types of Hacker Motivations," entry posted March 16, 2011, available from *blogs.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations/*, accessed on August 15, 2015.

28. Paul Rosenzweig, "The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence," *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy*, Washington, DC: National Academy of Sciences, 2010, pp. 256.

29. Gregory F. Treverton, "*Reshaping National Intelligence for an Age of Information*, Cambridge, UK: Cambridge University Press, 2003.

30. Bill Gertz, "'Deep Panda' Chinese cyber espionage gang linked to hack of 80 million Anthem health care records," available from *flashcritic.com/chinese-cyber-espionage-suspected-hack-health-care-provider-anthem/*, accessed on August 15, 2015.

31. Eric Talbot Jensen, "Cyber Deterrence," *Emory International Law Review* 2011, Vol. 26, p. 782, available from *law.emory.edu/eilr/_documents/volumes/26/2/symposium/jensen.pdf*, accessed on August 15, 2015.

32. Ellen Nakashima, "Security Firm finds link between China and Anthem hack," *The Washington Post*, available from *www.washingtonpost.com/news/the-switch/wp/2015/02/27/security-firm-finds-link-between-china-and-anthem-hack/*, accessed on August 15, 2015.

33. See Joseph S. Nye, Jr., "From bombs to bytes: Can our nuclear history inform our cyber future?" *Bulletin of the Atomic Scientists*, Vol. 69, No. 5, 2013, p. 8.

34. Robert Jervis, *The Logic of Images in International Relations*, Princeton, NJ: Princeton University Press, 1970.

35. See, for example, Mohd Aminul Karim, "Is Nuclear Deterrence Workable at the Brink Time in South Asia and Beyond?" *The Korean Journal of Defense Analysis,* Vol. 26, No. 1, 2014, pp. 35-49.

36. See John Rollins and Clay Wilson, *Congressional Research Service Report for Congress: Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, Washington, DC: U.S. Library of Congress, Congressional Research Service, 2007.

37. *Ibid.*, p. 4.

38. Dmitri Alperovitch, "Cyber Deterrence in Action? A story of one long HURRICANE PANDA Campaign," CrowdStrike, Executive Viewpoint, entry posted April 13, 2015, available from *blog.crowdstrike.com/cyber-deterrence-in-action-a-story-of-one-long-hurricane-panda-campaign/*, accessed on August 15, 2015.

39. Quoted in Cilluffo, Cardash, and Salmoiraghi, p. 6.

40. Iasiello, pp. 54-67.

41. Jensen. p. 788.

42. Therefore, it is likely that nuclear deterrence strategies—which, according to Jervis, are more useful for understanding crises than long-running disputes—are not the best sources to look at for identifying lessons to be used in developing doctrines for cyber-deterrence. See Jervis, *The Logic of Images in International Relations*, p. 293, on this weakness of nuclear deterrence theory.

43. See Brandon Valeriano and Ryan Maness, "Cyberwar and Rivalry: The Dynamics of Cyber Conflict between Antagonists, 2001-2011," *Journal of Peace Research,* Vol. 51, No. 3, pp. 347-360.

44. Richard Ned Lebow, "The Deterrence Deadlock: Is There a Way Out?" *Political Psychology*, Vol. 4, No. 2, 1983, pp. 333-354.

45. Barry Nalebuff, "Brinkmanship and Nuclear Deterrence: The Neutrality of Escalation," *Conflict Management and Peace,* Vol. 9, No. 2, Spring 1986, pp.19-30.

46. Jennifer Bradley, "Increase Uncertainty: The Dangers of Relying on Conventional Forces for Nuclear Deterrence," *Air and Space Power Journal*, July 1, 2015, pp. 72-85; Bernard Brodie, *The Absolute Weapon: Atomic Power and the World Order*, New York: Harcourt Brace, 1946, p. 76.

47. For more on the interagency approach, see Meir Elran and Gabi Siboni, "Establishing an IDF Cyber Command," *INSS Insight*, No. 719, The Institute for National Security Studies, July 8, 2015, available from *www.inss.org.il/index.aspx?id=4538&articleid=10007*, accessed on August 15, 2015. Although they describe the interagency context in Israel, their remarks may be relevant to the U.S. situation as well.

48. Reuters, "It's cyber war: guerilla tactics gain traction as a defense strategy," *Business Insurance*, available from *www.business-sinsurance.com/article/20150209/NEWS06/150209847*, accessed on August 15, 2015.

49. Peter T. Leeson and Christopher J Coyne, "The Economics of Computer Hacking," *Journal of Law, Economics and Policy*, 2005.

50. Gertz.

51. Jeremy Wagstaff, "Hunt for Deep Panda intensifies in trenches of U.S.-China Cyberwar," *Reuters*, available from *livenet-worknews.com/bz/article/100100100101242491*, accessed on August 15, 2015.

52. Cilluffo, Cardash, and Salmoiraghi, p. 7.

53. Drew Harwell and Ellen Nakashima, "China suspected in major hacking of health insurer," *The Washington Post*, available from *www.washingtonpost.com/business/economy/investigators-suspect-china-may-be-responsible-for-hack-of-*

*anthem/2015/02/05/25fbb36e-ad56-11e4-9c91-e9d2f9fde644_stor
.html*, accessed on August 15, 2015.

54. Kelly A. Gable, "Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent," *Vanderbilt Journal of Transnational Law*, Vol. 43, No. 1, p. 57.

55. See Clorinda Trujillo, "The Limits of Cyberspace Deterrence," *Joint Forces Quarterly*, Vol. 75, 4th qtr., 2014, pp. 43-52.

56. This posture is summarized in Trujillo, p. 45.

57. See Maurice Schiff, "The Problem of Illegal Immigration: Cooperation between Source and Host Countries," October 2013, article presented at the International Conference on "International labor mobility and inequality across nations," January 23-24, 2014, Clermont-Ferrand, FR, available from *www.ferdi.fr/sites/www.ferdi.fr/files/evenements/presentations/schiff.pdf*, accessed on August 15, 2015.

58. Barack Obama, "U.S. Cyber Operations Policy," Presidential Policy Directive-20 (PPD-20), Washington, DC: The White House, October 16, 2012, available from *fas.org/irp/offdocs/ppd/ppd-20.pdf*, accessed on August 15, 2015. President Obama makes this point in PPD-20, noting that "the United States Government shall work with private industry—through [Department of Homeland Security] DHS, [Department of Commerce] DOC and relevant sector-specific agencies—to protect critical infrastructure." He notes that certain types of responses are the purview only of the federal government, such as the ability to undertake offensive cyberoperations. The same can be said with reference to border security.

59. Quoted in John A. Mowchan, "On the Razor's Edge: Establishing Indistinct Thresholds for Military Power in Cyberspace," Program Research Project, Carlisle, PA: U.S. Army War College, 2012, pp. 6-7.

60. Trujillo, p. 46.

61. Wayne Cornelius and Idean Salehyan, "Does Border Enforcement Deter Unauthorized immigration? The Case of Mexican migration to the United States of America," *Regulation and Governance*, Vol. 1, No. 2, 2007, pp. 139-153.

62. Rosenzweig, p. 248.

63. John van Beveren, "A Conceptual Model of Hacker Development and Motivations," *Journal of E-Business,* Vol. 1, No. 2, December 2001, p. 3.

64. Siciliano.

65. Cilluffo, Cardash, and Salmoiraghi, pp. 4-5.

66. Mowchan.

67. My thinking here is influenced by my reading of Scott Helfstein *et al.*, "White Paper Prepared of the Secretary of Defense Task Force on DOD Nuclear Weapons Management: Tradeoffs and Paradoxes: Terrorism, Deterrence and Nuclear Weapons," *Studies in Conflict and Terrorism,* Vol. 32, No. 9, 2009, pp. 776-801.

68. Douglas F. Tippett, "Deterring Terrorism: A Framework for Making Retaliatory Threats Credible," Master's Thesis, Monterey, CA: Naval Postgreaduate School, available from *www.dtic.mil/dtic/tr/fulltext/u2/a514348.pdf*, accessed on August 15, 2015.

69. Paul F. Roberts, "Sony Hack Fits Pattern of Recent Destructive Attacks," *The Christian Science Monitor*, available from *www.csmonitor.com/World/Passcode/2014/1204/Sony-hack-fits-pattern-of-recent-destructive-attacks-video*, accessed on August 15, 2015.

70. Andrey Dulkin, "The Privilege Escalation Cycle and its Role in Russia's Anunak Cyber Attack," CyberArk, entry posted February 3, 2015, available from *www.cyberark.com/blog/privilege-escalation-cycle-role-russias-anunak-cyber-attack/*, accessed on July 29, 2015.

71. Dimitar Kostadinov, "The Cyber Exploitation Life Cycle," Infosec Institute, March 22, 2013, available from *resources.infosecinstitute.com/the-cyber-exploitation-life-cycle/*, accessed on August 15, 2015.

72. Nye, Jr., "From bombs to bytes," p. 10.

73. Obama.

74. Daniel Whiteneck, "Deterring Terrorists: Thoughts on a Framework," *Washington Quarterly*, Vol. 28, No. 3, p. 196, in Helfstein *et al.*, p. 782.

75. Quotes of Patrick M. Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," in Amir Lupovici, "Cyber Warfare and Deterrence: Trends and Challenges in Research," *Military and Strategic Affairs*, Vol. 3, No. 3, December 2011, p. 54.

76. This turn of events is described in Valeriano and Maness, p. 2.

77. See Group-IB and Fox-IT, "Anunak: APT Against Financial Institutions," report available from *https://www.fox-it.com/en/files/2014/12/Anunak_APT-against-financial-institutions2.pdf*, accessed August 2, 2015.

78. Lupovici, p. 57.

79. Cornelius and Salehyan.

80. Clement Guitton, "Criminals and Cyber Attacks: The Missing Link Between Attribution and Deterrence," *International Journal of Cyber Criminology*, Vol. 6, No. 2, 2012, pp. 1030-1043.

81. Paul N. Stockton and Michele Golabek-Goldman, "Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat," *Stanford Law and Policy Review*, Vol. 25, 2014, pp. 211-268.

82. *Ibid*.

83. Brittany Ann Morrisey, "Obama's Amnesty Legislation Misunderstood by Illegal Immigrants—Now DHS Needs Thousands of Pairs of Men's Briefs for Detained Illegal Immigrant Children," Reason.com, Hit & Run Blog, entry posted June 25, 2014, available from *reason.com/blog/2014/06/25/wanted-by-us-department-of-homeland-secu*, accessed on August 15, 2015.

84. Lupovici, pp. 49-62.

85. T.J. Espenshade, "Does the Threat of Border Apprehension Deter Undocumented US Immigration?" *Population and Development Review*, Vol. 20, No. 4, 1994, pp. 871-892.

86. *Ibid*.

87. Alexander George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice,* New York: Columbia University Press, 1974, p. 52-22, quoted in Jervis, *The Logic of Images in International Relations*, p. 307.

88. Thomas C. Schelling, *Arms and Influence*, New Haven: Yale University Press, 1966, p. 44.

89. Jervis, *The Logic of Images in International Relations*, p. 239.

90. See Sarah Bohn and Todd Pugatch, "U.S. Border Enforcement and Mexican Immigrant Location Choice," Discussion Paper No. 7842, December 2010, Bonn, Germany, IZA, available from *http://ftp.iza.org/dp7842.pdf*.

91. Cilluffo, Cardash, and Salmoiraghi, p. 16; See also, Rosenzweig, p. 245.

92. Cornelius and Salehyan.

93. For more on entanglement, see Scott Jasper, "Deterring Malicious Behavior in Cyberspace," *Strategic Studies Quarterly,* Spring 2015, p. 71.

94. See Rosenzweig.

95. Mowchan, p. 5.

U.S. ARMY WAR COLLEGE

Major General William E. Rapp
Commandant

*****

STRATEGIC STUDIES INSTITUTE
and
U.S. ARMY WAR COLLEGE PRESS

Director
Professor Douglas C. Lovelace, Jr.

Director of Research
Dr. Steven K. Metz

Author
Dr. Mary Manjikian

Editor for Production
Dr. James G. Pierce

Publications Assistant
Ms. Denise J. Kersting

*****

Composition
Mrs. Jennifer E. Nevil

U.S.ARMY®

THE UNITED STATES ARMY WAR COLLEGE

STRENGTH and WISDOM

FOR THIS AND OTHER PUBLICATIONS, VISIT US AT

http://www.carlisle.army.mil/

This Publication

SSI Website

USAWC Website